

REMARKS

Reconsideration and allowance are respectfully requested.

Claims 1-12, 16-27, and 31-42 stand rejected under 35 U.S.C. § 103 as being unpatentable over Asai and Hailpern. This rejection is respectfully traversed.

Asai describes a cluster server apparatus. Referring Figure 1, the Examiner equates the load distribution server 20 with the claimed load balancing device, the cache servers 101, 102, 10n with the plurality of proxy devices, the content server 30 with the file storage device, and the terminals 41, 42, 4n with the client devices. But as admitted by the Examiner, Asai does not disclose that the proxy devices (the cache servers of Figure 1) perform malware scanning of files stored within the file storage device. Indeed, Asai is entirely silent regarding the issue of malware scanning.

But malware scanning is an important feature of the present invention. The Federal Circuit *requires* consideration of the problem confronted by the inventors in determining whether it would have been obvious to combine references in order to solve that problem. *Northern Telecom, Inc. v. Datapoint Corp.*, 908 F.2d 931, 935 (Fed. Cir. 1990). Indeed, the Examiner must show reasons why one of ordinary skill in the art, confronted with the same problem as the inventor and with no knowledge of the claimed invention, would select the elements from the cited prior art references for combination in the manner claimed. See *In re Rouffet*, 149 F.3d 1350, 1357 (Fed. Cir. 1998).

As explained in the background portion of this application, malware scanning software is typically associated with the file storage device itself, and accordingly, if Asai's apparatus were to employ any malware scanning, it would likely be incorporated within the content server 30 itself. The problems with such an approach is the malware scanning can significantly undermine

the file server performance. Further, different software versions of the malware scanner typically have to be written for each different operating system that may be used by the content server.

The inventors realized that, irrespective of the operating system installed on the file storage device itself, most file access requests to such file storage devices are issued using a dedicated file access protocol, and the number of those dedicated file access protocols is less than the number of different operating systems used on the various file storage devices that are currently available (see page 4, line 17-21 of the application). Having appreciated this point, the inventors decided to provide a plurality of proxy devices, each coupled to the file storage device (see, e.g., the last two lines of claim 1), and each being arranged to perform malware scanning of files stored within the file storage device (see, e.g., line 2 of claim 1). The load balancing device is then arranged to apply a predetermined load balancing routine to determine to which proxy device to direct any particular access request (see, e.g., the penultimate paragraph of claim 1). Using this approach, malware scanning is not dependent on the file storage device vendor or on the operating system installed on that file storage device. As a result, the malware scanner may be used without modification within any computer network where the file access requests are issued using the dedicated file access protocol (see, e.g., page 5, lines 7-12, of the application).

The Examiner relies on Hailpern in an attempt to remedy Asai's deficiencies. Hailpern describes a load balancing proxy server system which is arranged to perform malware scanning. Hailpern's client devices access via the Internet content stored on content servers. As is known in such systems, a client device typically accesses the Internet via one or more proxy servers. For example, with reference to Figure 1, the client device 1220 accesses the Internet 1020 via proxy servers 1140, 1110 and 1100. Hailpern enables the proxy servers to collaborate when

performing virus checking based on meta-information associated with each data object retrieved via the Internet (column 1, lines 25-28). The meta-information enables any particular proxy server to keep track of processing performed by any other proxy server in the link between the client device and the Internet. As a result, those proxy servers can collaborate to perform virus checking. Considering the example above, if the proxy server 1100 has performed virus checking, then it can modify the meta-information prior to returning that data to the proxy server 1110, so that the proxy server 1110 does not repeat any virus checking performed by the proxy server 1100.

Hailpern's columns 11 to 14 describe that the meta-information can be taken into account when a particular proxy server is deciding whether to perform any virus checking. In particular, if a particular proxy server is very busy, and it knows that a proxy server further down the chain has the capability to perform the virus checking, it can decide not to perform the virus checking itself. Instead, the proxy server may let the proxy server further down the chain perform that virus checking, thereby enabling a certain balancing of the load. But this approach to load balancing employed by Hailpern is very different from the approach invented by the inventors in this case.

Indeed, Hailpern's system lacks features recited in the independent claims. For example, Hailpern lacks a load balancing device arranged (1) to intercept an access request issued to the file storage device and (2) *to apply a predetermined load balancing routine to determine to which proxy device to direct that access request*. Instead, the sequence of proxy servers needed to process an access request in Hailpern is already predetermined and is client dependent. As an example, the client 1220 must access the Internet 1020 via one or more of the proxy servers

1140, 1110 and 1100, and the proxy server 1100 is the only proxy server allowed to actually access the Internet.

In addition, none of Hailpern's proxy servers is *coupled to the file storage device*, since Hailpern's file storage device resides somewhere else over the Internet. In contrast, each of the claimed proxy devices that the load balancing logic can direct the access request to is coupled to the file storage device. See for example the last line of claim 1: "each proxy device being coupled to the file storage device."

The claimed load balancing logic "intercept[s] an access request issued to the file storage device" and "determine[s] which proxy device to direct that access request" (quoted from claim 1). Thereafter, the selected single proxy device performs the required malware scanning prior to the access being allowed to proceed. Hailpern's predetermined number of proxy servers, in contrast, are used to access the Internet in order to retrieve a file, and then only once the file has been retrieved, is any malware scanning performed. Hailpern does apply a predetermined load balancing routine in order *to determine to which proxy device to direct the access request to*. The only load balancing provided in Hailpern is through the use of some meta-information to decide which of multiple proxy servers in the chain may perform virus checking.

Thus, even if Hailpern's teachings could be combined with Asai, their combination would not result in the combination of features recited in claim 1 and the other independent claims 10, 16, 31 and 40. And given the very different technology and focus of Hailpern and Asai, it is difficult to see how a person of ordinary skill in the art would have been motivated to combine them as the Examiner proposes. Notably, Hailpern fails to provides a teaching that would have directed a person skilled in the art to provide for malware scanning within any of Asai's cache servers 101, 102, ..., 10n. The Examiner also fails to show that either Asai or Hailpern

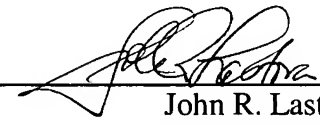
recognized or was confronted with the same problem as the instant inventors. Absent that recognition, it is clear that the Examiner's attempted combination lacks the requisite motivation. The *Rouffet* Court warned against "rejecting patents solely by finding prior art corollaries for the claimed elements" because that would "permit an Examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art." *In re Rouffet*, 149 F.3d at 1357. That approach was found by the Federal Circuit to be "an illogical and inappropriate process by which to determine patentability." *Sensonics v. Aerosonic Corp.*, 85 F.3d 1566, 1570 (Fed. Cir. 1996).

The application is in condition for allowance. An early notice to that effect is solicited. If the Examiner believes that a telephone conference would be helpful in advancing the prosecution of this application, the Examiner is kindly invited to contact the undersigned at the telephone number noted below.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By:



John R. Lastova
Reg. No. 33,149

JRL:sd
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100